

**AFFIDAVIT IN SUPPORT OF A  
SEARCH WARRANT APPLICATION**

I, Stephanie L. Rattigan, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and am currently assigned to the FBI Boston Division - Portland, Maine Resident Agency, where I am an Agent on the Southern Maine Gang Task Force. I have been employed as an FBI Special Agent for over 7 years. I have been trained in various aspects of law enforcement, to include specialized training in evidence collection as a member of the FBI's Evidence Response Team. I have investigated various types of violent crimes in the States of New Jersey and Maine, to include crimes involving fugitives, criminal enterprises, firearms, bank robberies, kidnappings, narcotics, violent crimes against children, crimes aboard aircrafts, and crimes on the high seas. I have participated in the execution of numerous search and arrest warrants, authorizing the search of residences and the search and seizure of computers, computer equipment, software, and electronically stored information.

2. I make this affidavit in support of an application for an anticipatory search warrant under Federal Rule of Criminal Procedure 41(b)(1) to search for and seize any evidence regarding potential violations of 18 U.S.C. § 2252A(a)(1) (transportation of child pornography), 18 U.S.C. § 2252A(a)(2)(A) (receipt and attempted receipt of child pornography) and 18 U.S.C. § 2252A(a)(5)(B) (possession and attempted possession of child pornography) (collectively the "Subject Offenses"). Specifically, I seek authorization to search for and seize the items more fully set forth in Attachment B.

3. These items are believed to be contained in information from MEGA Ltd. (“MEGA”) that is associated with the accounts afuentedom@protonmail.com, frostjako@gmail.com, and shrngsvdgrl@gmail.com (the “Subject Accounts”) and the folder\_mega.nz/folder/TooGiahA#1is3xMlinkPRBAxmjLwmng (the “Subject Folder”). As explained herein, I believe that the Subject Accounts and the Subject Folder contain child pornography, as that term is defined in 18 U.S.C. § 2256. The contents of the Subject Accounts and the Subject Folder are currently being stored on servers in New Zealand, but I anticipate downloading their contents to computer media in the possession of the FBI in the District of Maine, as more fully set forth in Attachment A.

4. The facts set forth in this affidavit come from my direct involvement in this investigation, my training and experience, and information I have obtained from law enforcement personnel and witnesses.

### **BACKGROUND ON MEGA**

5. MEGA is a corporation that provides cloud storage, file hosting, and communications services through its website, <https://mega.io>, and its mobile application, which is available for download for Apple users on the App Store and for Android users on the Google Play Store. MEGA is incorporated in New Zealand, and its headquarters are located at Level 21, Huawei Centre, 120 Albert Street, Auckland, New Zealand. On information and belief, MEGA’s computer servers are located in New Zealand.

6. A MEGA user can sign up for an account with a valid email address, which becomes the user’s MEGA username. MEGA provides users with a certain amount of free data storage; if a user wants more storage, the user can pay for it. Users can access

MEGA through the internet from most major devices and platforms, from anywhere in the world. For example, a user may take a photo with their cell phone, upload that photo to MEGA, and then delete the photo from their cell phone. The photo now resides on MEGA's servers. The user then can access their MEGA account from a different device and download the photo to that device.

7. A MEGA user can designate a folder (or folders) on their device, which MEGA synchronizes with the user's account. As a result, that same folder with those same contents will appear on both the user's device and their MEGA account. Files placed in that folder are accessible through MEGA's website as well as MEGA's mobile application. A MEGA user also can share folders with other people by sending links, which gives the recipients the ability to access the contents of those folders, including any files placed in them. Another feature of MEGA is "MegaChat," which allows users to exchange messages and participate in audio, video, and group chats.

8. Data associated with a MEGA account is stored on MEGA's servers in an encrypted format. Data also is transmitted in an encrypted format between MEGA's servers and users' devices. In addition, messages between users are transmitted in an encrypted format within MEGA's server network. MEGA's server architecture means that data is encrypted in such a way that makes it mostly inaccessible. Data is encrypted on the user side using encrypted key(s) that users control. This means that, barring exceptional circumstances, MEGA does not have the ability to decrypt a user's folders, files, or messages, and MEGA is usually unable to provide data in a usable format to third parties.

9. One such exceptional circumstance involves child sexual abuse material (CSAM),<sup>1</sup> for which MEGA maintains a zero-tolerance policy. When MEGA receives a report about CSAM on its servers, MEGA disables the link for the folder or chat and closes the user's account. MEGA also voluntarily discloses all available information, including account details and the contents of the link, to New Zealand's Department of Internal Affairs ("NZ DIA"). Depending on the format of the link as determined by the user, NZ DIA may be able to review the contents of that the link and share that content with law enforcement when necessary.

10. As explained herein, the contents of a folder stored on Mega's servers may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. This information may indicate who controlled, used, or accessed a particular folder. For example, individual files in a particular folder that were uploaded or downloaded (and the metadata associated with the foregoing, such as date and time) may indicate who controlled, used, or accessed the folder during the relevant period. Individual files in the folder also may reveal the identity of other victims and the underlying time frames in which they were victimized (e.g. folders with victim data and the metadata associated with file transfers). Additionally, the contents of the folder may provide relevant insight into the owner or user's state of mind as it relates to the offenses under investigation.

---

<sup>1</sup> The term "CSAM" is used interchangeably herein with the term child pornography and refers to material that meets the definition of child pornography set forth in 18 U.S.C. § 2256(8).

For example, information in the folder may indicate the owner or user's motive and intent to commit a crime (e.g. communications relating to the crime) or consciousness of guilt (e.g. deleting communications to conceal them from law enforcement).

### **PROBABLE CAUSE**

11. In or about May of 2022, FBI Headquarters, Criminal Investigative Division, Child Exploitation Operational Unit (CEOU) conducted an operation targeting websites and applications dedicated to the distribution, advertisement, and production of CSAM.

12. On or about May 3, 2022, an FBI Online Covert Employee (OCE) was connected to the internet in an online undercover capacity. A software program was used to record the online activity, chats, and videos identified within the platforms Wickr and MEGA.

13. Wickr is an end-to end encrypted service that enables secure one-to-one and group messaging, voice and video calling, file sharing, and screen sharing.

14. As noted above, MEGA is a secure cloud storage service with end-to-end encryption that allows the upload of files to a cloud-based server. MEGA accounts come with free cloud storage upon creation. A MEGA user does not need to create an account to view or access a link; they can simply download the link and can share that link with anyone.

15. On May 3, 2022, the OCE entered the Wickr chat and observed Wickr user [mcmxcii6@protonmail.com](mailto:mcmxcii6@protonmail.com) share a MEGA link to the Subject Folder in the Wickr group chat titled "This group is now inactive."

16. The following titled chat rooms were visible on the left side panel within the Wickr group chat screenshot taken by the OCE:

- pedo lives matter
- we love little1's
- hc pedo babies and toddlers
- anarchy porn group
- kids + teens zoo
- no limits
- the abducters
- perv clubhouse 2021
- nepi rape and abuse
- younger girl the better
- jailbait share no preteen
- CopAFeel
- WTF
- braces
- braces 2.0 in cleaning
- users from vip hentai
- reactions
- VIP – verified no rules
- cumsluts
- tiny girls – in cleaning
- abandoned perv club
- hardcore (pain, violence...)

17. The above-described MEGA link shared within the group chat contained numerous CSAM videos.

18. Within the screen recording captured by the OCE, there were approximately 519 videos of pre-pubescent females performing sexual acts on themselves or a male, or posing in a lascivious manner.

19. Of the approximately 519 videos, the OCE downloaded approximately six full sample videos ranging from 12 seconds to 5 minutes and 42 seconds.

20. One of the sample videos downloaded by the OCE showed a pre-pubescent brunette-haired female, wearing a white sweatshirt, mustard-colored pants, and white underwear, holding a beige cat. In the video, the minor female takes off her clothes and manipulates her own vagina by pulling it open wider and posing in a sexual nature. The minor female then pulls a male's penis out of his pants and begins to rub it. In the video, the male attempts to put his penis near the female's mouth, and the female exclaims "yuck" and turns away. The video ends with the female wiping the male's penis with her sweatshirt and beginning to lick the top of his penis. The video is 4 minutes and 27 seconds in length. The male's face is not visible in the video. A screenshot taken from this video is submitted herewith under seal as Exhibit 1.

21. Another video downloaded by the OCE shows a pre-pubescent blonde-haired female on a chair in front of a computer, rubbing her vagina with liquid on it. The video ends with the female trying to insert a blue object into her anus. The video is one minute in length. A screenshot taken from this video is submitted herewith under seal as Exhibit 2.

22. Finally, another video downloaded by the OCE shows a pre-pubescent brunette-haired female inserting an object into her vagina and then licking the object. The video was 5 minutes and 42 seconds in length. A screenshot taken from this video is submitted herewith under seal as Exhibit 3.

23. After the OCE downloaded the above-described videos, a request was sent to NZ DIA, which is the foreign law enforcement point of contact for MEGA. NZ DIA returned an Excel spreadsheet with the Basic Subscriber Information (BSI) of the owner



of the MEGA account that created the above-described link to the Subject Folder. The information provided was as follows:

E-mail: [afuentedom@protonmail.com](mailto:afuentedom@protonmail.com)

First name: Fuent

Last name: Dom

24. MEGA also provided various internet protocol (IP) addresses that were associated with the link owner. On May 11, 2022, CEOU served an administrative subpoena on Charter Communications, Inc. for the following IP addresses:

- a. 2603:7081:2341:9c00:49bf:1110:23bb:7430 used on February 11, 2022 at 12:24:21 UTC;
- b. IP Address: 2603:7081:2341:9c00:a869:95f4:1ad3:1a06 used on February 9, 2022 at 12:51:15 UTC;
- c. IP Address: 2603:7081:2341:9c00:6055:e04:3c4b:df24 used on February 8, 2022 at 10:42:10 UTC.

25. Charter Communications subsequently provided the following information about the subscriber:

Name: Aaron Coy

Address: 48 State Street, Apt. 101, Biddeford, ME 04005-5272

Email: [aaronwcoy@gmail.com](mailto:aaronwcoy@gmail.com)

Telephone: 208-201-9417

Connection Date: 06/24/2019

Account Status: Active

26. On June 28, 2022, CEOU performed open-source research and analysis on the identifiers associated with the subscriber and identified the following individual:

Aaron William Coy, DOB: x/x/1992; SSAN: xxx-xx-7414;

Current address: 48 State St, Apt 101, Biddeford, ME;

E-mail addresses: [aaroncoy1309@hotmail.com](mailto:aaroncoy1309@hotmail.com); [aaroncoy@msn.com](mailto:aaroncoy@msn.com) and [cy2rich@yahoo.com](mailto:cy2rich@yahoo.com).



27. On August 1, 2022, CEOU sent a lead to the FBI Boston Division, Portland, ME Resident Agency with the above information and requested that agents locate the MEGA user who shared the link containing CSAM.

28. On May 17, 2023, I obtained a search warrant for Aaron Coy's residence and vehicle based on an ongoing FBI investigation regarding suspected violations of 18 U.S.C. § 2252 (certain activities related to material involving the sexual exploitation of minors) and 18 U.S.C. § 2252(A)(1).

29. During the execution of the search warrant at Coy's residence, I interviewed Coy. During this interview, Coy admitted to having and using the Wickr and MEGA platforms, and sending and opening MEGA links within chats. Coy also admitted to viewing images of young girls and trading links containing CSAM for the purpose of receiving links in return. Coy said that pornography was an "addiction" for him.

30. On November 17, 2023, the forensic examination of Coy's devices was completed. According to the forensic examination report, Coy's cellular telephone contained the credentials to a different MEGA account than the one which had shared the link to the Subject Folder. This MEGA account had the username shrngsvdgrl@gmail.com and a password of FuckSlut7224!

31. On February 7, 2024, I contacted MEGA for additional information about the Subject Folder. A MEGA employee referred me to NZ DIA. A Senior Investigator from the NZ DIA Digital Child Exploitation Team subsequently confirmed the following information for me: (a) he had accessed the Subject Folder and account information for afuentedom@protonmail.com, (b) the user of this account created the MEGA link to the Subject Folder that I had provided, (c) that link provided access to a folder containing

519 files (i.e., the Subject Folder), the majority of which appeared to be CSAM, (d) the [afuentedom@protonmail.com](mailto:afuentedom@protonmail.com) account has a total of 948 files, and (e) the user of the account had deleted a total of 21,812 files, which MEGA can recover and provide.

32. When MEGA provided the Basic Subscriber Information for the MEGA account that shared the link to the Subject Folder in 2022, MEGA did not know the password associated with that account. On May 15, 2024, I contacted NZ DIA and asked them to check whether the password Fuckslut7224! (which we had found on Coy's cellphone) was the password to the MEGA account of user [afuentedom@protonmail.com](mailto:afuentedom@protonmail.com). In my experience, people often re-use the same password, or variations of the same password, for different online accounts and applications, to make it easier to remember the password.

33. On May 15, 2024, A Senior Investigator from the NZ DIA Digital Child Exploitation Team told me that he had asked MEGA to check the following passwords against all MEGA accounts:

Fuckslut7224!  
Fuckslut7224  
fuckslut7224!  
fuckslut7224

However, according to the Senior Investigator, none of these passwords was a match for any MEGA account (including the account that had shared the link to the Subject Folder).

34. On June 13, 2024, I contacted NZ DIA and asked investigators to search again using the password of FuckSlut7224! (with a capital 'S').



35. On June 13, 2024, a Senior Investigator from the NZ DIA Digital Child Exploitation Team reported that the password FuckSlut7224 (without the '!') worked for the account of [afuentedom@protonmail.com](mailto:afuentedom@protonmail.com) (i.e., the account that had shared a link to the Subject Folder). The Senior Investigator also informed me that if legal authority were provided, the NZ DIA would be able to access and provide the Subject Folder currently held in the account and recover an additional 21,812 files that had been previously deleted by the account owner.

36. The Senior Investigator also told me that when the NZ DIA had been initially contacted and asked about the email address [afuentedom@protonmail.com](mailto:afuentedom@protonmail.com), NZ DIA had asked MEGA to look for related accounts associated with that particular MEGA account.<sup>2</sup> However, according to the NZ DIA Senior Investigator, it appears that MEGA never sent NZ DIA the results of that search. In this case, it turns out that MEGA was able to identify two additional accounts that had accessed MEGA using the same device that was used to access the [afuentedom@protonmail.com](mailto:afuentedom@protonmail.com) account. Those accounts were [frostjako@gmail.com](mailto:frostjako@gmail.com) and [shrngsvdgrl@gmail.com](mailto:shrngsvdgrl@gmail.com).<sup>3</sup> The Senior Investigator told me

---

<sup>2</sup> MEGA has the ability to look for MEGA accounts that are related to each other by device or supercookie. A supercookie is a data file that is inserted into an HTTP header to track a user's browsing habits. It is also known as a unique identifier header (UIDH). Supercookies are stored on a user's computer indefinitely and are difficult to remove. They can collect information such as a user's browsing history, login details, and ad targeting information. Supercookies are stored in a different part of the hard drive than regular cookies. They're also more persistent than regular cookies. Supercookies can be used to track users across multiple websites, regardless of which browser they are using. They can also be used to infiltrate networks and identify a user's network connection from others.

<sup>3</sup> As noted above in Paragraph 30, the FBI's forensic examiner found credentials for this second MEGA account stored in Aaron Coy's cell phone.

that MEGA also confirmed that the password FuckSlut7224! is the correct credential for the account [shrngsvdgrl@gmail.com](mailto:shrngsvdgrl@gmail.com).

37. According to the NZ DIA Senior Investigator, the [shrngsvdgrl@gmail.com](mailto:shrngsvdgrl@gmail.com) account does not have any files currently stored in the account Cloud Drive. However, MEGA confirmed that it is able to provide 5978 deleted files from this account, which the NZ DIA can recover and provide to the FBI. The Senior Investigator also informed me that the account also reports two chat sessions. Chat sessions are consistent with the trading of CSAM described by Coy.

38. The accounts associated with [frostjako@gmail.com](mailto:frostjako@gmail.com) and [shrngsvdgrl@gmail.com](mailto:shrngsvdgrl@gmail.com) were created from the same device, and with an identical or similar password that was created by the [afuentedom@protonmail.com](mailto:afuentedom@protonmail.com) account, which was linked to Coy through his Charter Communications IP address.

39. Based on the foregoing, I submit that probable cause exists to believe that Coy used MEGA—including its encrypted features and its foreign location—to possess or receive images of child pornography that he obtained via the internet.

40. The information about, and contents of, the Subject Folder and Subject Accounts are currently believed to be stored on servers located in New Zealand. It is my understanding that the Fourth Amendment's warrant requirement generally does not apply to locations outside the territorial jurisdiction of the United States, *see United States v. Stokes*, 726 F.3d 880, 890-93 (7th Cir. 2013), and that a warrant issued under Federal Rule of Criminal Procedure 41 would not authorize the search of a server located in New Zealand under these circumstances. *See also United States v. Verdugo-Urquidez*, 494 U.S. 259, 274 (1990) (describing a warrant issued by a United States

magistrate as “a dead letter outside the United States”). Therefore, I seek this warrant out of an abundance of caution, to be certain that the examination of the Subject Folder and Subject Accounts’ contents, if downloaded to computer media in the possession of the FBI located in the District of Maine, will comply with the Fourth Amendment and other applicable United States laws.

### **CONDITION REQUIRED PRIOR TO EXECUTION**

41. The FBI plans to attempt to access the Subject Folder and Subject Accounts using the instructions provided by New Zealand’s Department of Internal Affairs. If such access is successful, the FBI intends to download any available information about the Subject Folder and Subject Accounts onto computer media in the possession of the FBI located in the District of Maine. The downloaded information may include, but is not limited to, information about individual files, communications, and users associated with the Subject Folder and Subject Accounts.

42. I am seeking permission to search the Subject Folder and Subject Accounts and following the triggering event of the download of said information by the FBI into the District of Maine, as described in Attachment A, and to seize the items and information described in Attachment B.

43. Because this warrant seeks permission only to examine information on computer media in law enforcement’s possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

### **CONCLUSION**



44. I respectfully submit that there is probable cause to believe that evidence of the Subject Offenses, as more fully set forth in Attachment B, is currently located in the Subject Folder and Subject Accounts identified by the New Zealand Department of Internal Affairs.



Respectfully submitted,

Stephanie L. Rattigan  
Stephanie L. Rattigan  
Special Agent, FBI

Sworn to telephonically and signed  
electronically in accordance with the  
requirements of Rule 4.1 of the Federal Rules  
of Criminal Procedures

Date: Nov 13 2024

City and state: Portland, Maine

  
  
Judge's signature  
Karen Frink Wolf, U.S. Magistrate Judge  
Printed name and title